

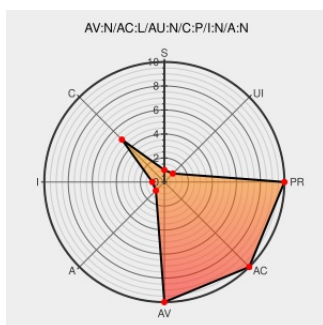


# CVE-2004-1743

Published on: 08/24/2004 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:09 PM UTC

## CVE-2004-1743

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Efs Web Server](#) from [Efs Software](#) contain the following vulnerability:

Easy File Sharing (EFS) Webserver 1.25 allows remote attackers to view arbitrary files via an HTTP request for the disk\_c virtual folder.

CVE-2004-1743 has been assigned by [M](#) [cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access  
Vector

**NETWORK**

Access  
Complexity

**LOW**

Authentication

**NONE**

Confidentiality  
Impact

**PARTIAL**

Integrity  
Impact

**NONE**

Availability  
Impact

**NONE**

## CVE References

Description

Tags

Link

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)  
[text/html](#)

[XF easyfilessharing-obtain-info\(17109\)](#)

SecurityTracker.com Archives - Easy File Sharing Web Server Discloses All Files on the Disk to Remote Users

[Exploit](#)  
[Vendor Advisory](#)  
[securitytracker.com](#)  
[text/html](#)

[SECTrack 1011045](#)

Easy File Sharing Web Server Access Control Bypass Vulnerability

[Vendor Advisory](#)  
[cve.report \(archive\)](#)  
[text/html](#)

[BID 11034](#)

Secunia - Advisories - Easy File Sharing Web Server Exposure of Sensitive Information

[Vendor Advisory](#)  
[web.archive.org](#)  
[text/html](#)

[SECUNIA 12372](#)

Contact Support

[Exploit](#)

[MISC www.gulftech.org/?](#)

Vendor Advisory

www.gulftech.org

text/html

node=research&article\_id=00045-08242004

'Easy File Sharing Webserver v1.25 Vulnerabilities' - MARC

marc.info

text/html

BUGTRAQ 20040824 Easy File Sharing Webserver v1.25 Vulnerabilities

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

| Type        | Vendor                       | Product                        | Version | Update | Edition | Language |
|-------------|------------------------------|--------------------------------|---------|--------|---------|----------|
| Application | <a href="#">Efs Software</a> | <a href="#">Efs Web Server</a> | 1.2     | All    | All     | All      |
| Application | <a href="#">Efs Software</a> | <a href="#">Efs Web Server</a> | 1.25    | All    | All     | All      |
| Application | <a href="#">Efs Software</a> | <a href="#">Efs Web Server</a> | 1.2     | All    | All     | All      |
| Application | <a href="#">Efs Software</a> | <a href="#">Efs Web Server</a> | 1.25    | All    | All     | All      |

cpe:2.3:a:efs\_software:efs\_web\_server:1.2:\*:\*:\*:\*:\*:

cpe:2.3:a:efs\_software:efs\_web\_server:1.25:\*:\*:\*:\*:\*:

cpe:2.3:a:efs\_software:efs\_web\_server:1.2:\*:\*:\*:\*:\*:

cpe:2.3:a:efs\_software:efs\_web\_server:1.25:\*:\*:\*:\*:\*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→